Australian Government

Australian Security Intelligence Organisation

CORPORATE PLAN 26 30



ASIO

Securing Australia—protecting its people

© Commonwealth of Australia 2026

With the exception of the Coat of Arms, this publication is licensed under a Creative Commons Attribution 3.0 Australia Licence.

All material presented in this publication is provided under a Creative Commons BY Attribution 3.0 Australia licence (https://creativecommons.org/licenses/by/3.0/deed.en).



The details of the relevant licence conditions are available on the Creative Commons website (accessible using the link provided) as is the full legal code for the Creative Commons BY Attribution 3.0 Australia licence (https://creativecommons.org/licenses/by/3.0/legalcode.en).

Use of the Coat of Arms

The Commonwealth Coat of Arms is used in accordance with the December 2014 *Commonwealth Coat of Arms: information and guidelines*, published by the Department of the Prime Minister and Cabinet and available online (https://pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

Contact us

Phone

General inquiries 1800 020 648

Media inquiries 02 6249 8381

Email

media@asio.gov.au

Post

GPO Box 2176, Canberra ACT 2601

Acknowledgement of Country

The Australian Security Intelligence Organisation acknowledges the Traditional Custodians of Country throughout Australia and their continuing connection to land, waters and community. We pay our respects to all Aboriginal and Torres Strait Islander peoples, their cultures and to their Elders past, present and emerging.

Director-General's introduction

I am pleased to present the ASIO Corporate Plan for 2026–27 to 2029–30, as required under section 35(1)(b) of the *Public Governance, Performance and Accountability Act 2013*.

ASIO protects Australia and Australians from threats to their security. In a dynamic, diverse and degrading security environment, our mission has never been more important – or more challenging.

Our Corporate Plan lays out how we will address the challenge, and how we will measure our performance.

Counter-terrorism

Politically motivated violence – which includes terrorism – remains one of Australia's principal security concerns.

Obviously, the heartbreaking and senseless terrorist attack at Bondi is a stark example of the persistent threat of violent extremism.

On behalf of ASIO I acknowledge the deep pain and grief of the families, friends and community of those killed and injured in the tragedy.

I acknowledge those who ran towards danger to help. And I acknowledge my staff and our law enforcement partners who worked around the clock in the days, weeks and months following the attack, and continue to advance our counter-terrorism mission.

As a nation, we are rightly shocked by any act of terrorism. But unfortunately, we should not be surprised.

A national terrorism threat level of PROBABLE means an attack or attack planning is more likely than not. As I noted in our 2025 Corporate Plan:

> *"Politically motived violence is raising the temperature of the security environment and making acts of terrorism more likely."*

In Australia – and in other western democracies – grievance is growing, social cohesion is straining, trust in institutions is declining, and intolerance is spreading.

At the same time, traditional transnational terrorist groups such as Islamic State, al-Qa'ida and their affiliates are exploiting permissive spaces to revive and renew their capabilities. While these groups have demonstrated an intent and capability to conduct attacks in foreign countries, the greatest threat in Australia is still an individual or small group using an easily obtained weapon and moving to violence with little or no warning.

ASIO will continue to prioritise its counter-terrorism mission. Key features of the contemporary security environment – including online radicalisation and the spikes in grievance and intolerance – require a whole-of-community response.

Counter-intelligence

Espionage and foreign interference are our other principal security concerns.

Great power competition is driving a relentless hunger for strategic advantage and an insatiable appetite for inside information.

Based on what ASIO is identifying and investigating, more Australians are being targeted for espionage and foreign interference than ever before.

Multiple nations – even some we consider friendly – are seeking to covertly understand and shape Australia's politics and decision-making, our alliances and partnerships, and our economic and policy priorities.

Increasingly, foreign intelligence services are broadening their collection requirements beyond the traditional categories, aggressively targeting science and technology, as well as public and private sector projects, negotiations and investments that might give foreign companies a commercial advantage. This includes Antarctic research, green technology, critical minerals and rare earths extraction and processing.

AUKUS remains a priority for intelligence collection. ASIO has identified foreign services unsuccessfully seeking to obtain sensitive information about the capabilities and how Australia intends to use them.

At the same time, hostile nation states are persistently trying to penetrate the networks of Australia's critical infrastructure providers. ASIO assesses the hackers want to maintain persistent undetected access that would allow them to conduct sabotage at a time and moment of their choosing.

Over the period of this Corporate Plan, ASIO will maintain our high-tempo investigative and operational activities to detect and counter espionage, foreign interference and sabotage threats.

Top Secret–Privileged Access

For foreign powers targeting Australia, security-cleared personnel with privileged access to information are an attractive means by which to enable acts of espionage.

The TS-PA Vetting Authority plays a critical role protecting Australia from the threat of espionage and foreign interference. It ensures security clearances are centrally managed to a consistent high standard of trust, and that only appropriately cleared individuals have access to our nation's most sensitive information and assets.

Last year marked a significant milestone for the National TS-PA Capability, with the TS-PA Vetting Authority now established and centralised within ASIO. In 2026–27, ASIO will continue to build the capacity needed to meet growing demand for TS-PA security clearances across the Commonwealth. We will deliver to the agreed standard of continuous assurance while protecting Australia's workforce from threats targeting our most sensitive information, capabilities and assets.

Influence and impact

The ASIO Act empowers ASIO to collect, assess and *communicate* intelligence.

The scale and sophistication of the threats facing Australia requires ASIO to be proactive in the way it communicates with government, business, academia, industry and the public.

Over the period of this Corporate Plan, ASIO will leverage our capabilities and intelligence to continue to provide actionable insights and impactful advice to help make Australia a more resistant and resilient target.

We will do this through classified reporting, public statements and speeches, and targeted campaigns that address specific security concerns.



Mike Burgess AM
Director-General of Security

Deputy Director-General Intelligence Service Delivery
The DDG/ISD-designate will commence in the role in the second half of 2026



Lisa Alonso Love
Deputy Director-General Enterprise Service Delivery



Gus Gilmore
Deputy Director-General Vetting Service Delivery

Conclusion

Despite the dynamic, diverse and degrading threat environment, Australia should not be insecure about its security.

The threats are not insurmountable. Foreign intelligence services are not invincible. A terrorism threat level of PROBABLE does not mean inevitable.

We can and should have confidence in our ability to respond.

ASIO and our law enforcement partners have disrupted 31 major terrorist plots since 2014.

In 2026–27, ASIO will carefully prioritise its resources against diverse threats to ensure we remain well placed to secure Australia and protect its people.



Mike Burgess AM
Director-General of Security

ASIO Corporate Plan 2026–30

PURPOSE

ASIO protects Australia and Australians from threats to their security.

SECURITY INTELLIGENCE OUTCOMES

COUNTER-INTELLIGENCE

Protect Australia and Australians from espionage, foreign interference and sabotage through early detection of threats, and action to address harm, build resilience and deter future threats.

COUNTER-TERRORISM

Protect Australia and Australians from violent extremism by anticipating threats and responding to changes in the security environment.

CAPABILITIES

PEOPLE

ASIO's people are fundamental to our business, and our culture enables their success. We recognise the importance of attracting, developing and retaining our diverse, imaginative and curious workforce. We empower and support staff to achieve their full potential, fostering leadership at all levels.

PRACTICES

ASIO acts with authority to stay ahead of our adversaries through disciplined business processes and tradecraft. Our practices enable intelligence-led and risk-based planning, operational decision-making, prioritisation, and ensure the effective and efficient use of resources. We adapt and lead in developing security practices, operating with integrity and in compliance with the law.

PARTNERSHIPS

Security is a shared responsibility and ASIO delivers its mission through strong partnerships. These relationships span government, including the National Intelligence Community, law enforcement, our state and territory partners, international counterparts, industry, academia and the Australian public. We contribute our capabilities and experience to enhance the collective response to government.

CONTEXT AND EXTERNAL DRIVERS

Security outlook

Geopolitical shifts

Technology advancement



INFLUENCE AND IMPACT

Leverage our capabilities and insights to help stakeholders better understand, identify and manage sophisticated security threats.

TOP SECRET–PRIVILEGED ACCESS VETTING

Deliver highly assured and transferable security clearances to Australia's highest-cleared workforce to enable the government to better manage and combat threats to its information, people and assets.

TECHNOLOGY

ASIO uses a human-led, data-driven, technology-enabled approach to understand and respond to threats. We embrace new technologies, leverage automation, and seize opportunities to innovate, including working with Australian industry partners. ASIO's capability programs ensure we keep in step with rapidly changing technologies and practices to provide the security assurance Australians expect.

ASSURANCE

Trust, governance, accountability and transparency are fundamental for achieving intelligence outcomes. Our risk, compliance and governance frameworks ensure we act within the letter and the spirit of the law. ASIO delivers on its mission using rigorous internal controls, embracing independent external oversight while ensuring ASIO is free from any influences or considerations not relevant to its functions.

Legislative and policy environment

Community expectations

Fiscal and labour market conditions

Agency overview

ASIO's role

ASIO's purpose is to protect Australia and Australians from threats to their security.

ASIO's functions are set out in section 17 of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act).

'Security' is defined in section 4 of the ASIO Act as the protection of Australia and its people from:

- espionage;
- sabotage;
- politically motivated violence;
- promotion of communal violence;
- attacks on Australia's defence system; or
- acts of foreign interference;

whether directed from, or committed within, Australia, or not; and

- the protection of Australia's territorial and border integrity from serious threats.

The definition of security also extends to the carrying out of Australia's responsibilities to any foreign country in relation to matters noted above.

ASIO achieves its purpose by obtaining, correlating, evaluating and communicating intelligence relevant to security.

ASIO cannot just respond to threats, it must anticipate them.

ASIO also has a function to obtain foreign intelligence within Australia.

We protect Australia and Australians by:

- understanding our security environment and identifying security threats;
- providing threat and security advice to harden the environment against future threats; and
- working with partners to disrupt threats and reduce harm.

We communicate and advise to inform operational action, government decision-making, policy development and community resilience. We work with other agencies and authorities to achieve outcomes that protect Australia's national interests.

The Director-General of Security is an independent statutory office holder with specific responsibilities under the ASIO Act to ensure the work of the Organisation is limited to what is necessary to discharge ASIO's functions.

The Director-General of Security is responsible for ensuring ASIO is free from any influences or considerations not relevant to its functions, and to ensure nothing is done that might lend colour to any suggestions ASIO seeks to further or protect the interests of any section of the community.

ASIO's operating context and external drivers

Australia's security environment is dynamic, diverse and degrading.

Evolving security environment

Australia is operating in an era of strategic surprise, facing a rising storm of concurrent security threats. We have moved beyond a landscape of isolated risks into a period of multifaceted instability, where state-sponsored aggression and domestic volatility are intersecting. At the centre of this storm are the acute pressures of espionage, foreign interference, and politically motivated violence; however, the perimeter is expanding. We are now seeing surges of communal violence, sabotage, and threats to Australia's Defence system. Driven by a degrading global security environment and accelerated by new technologies, these intersecting threats represent a systemic challenge to our national security.

The enduring ability of transnational terrorist groups to inspire politically motivated violence in Australia was tragically demonstrated in Bondi in 2025. This threat persists, alongside new actors, ideologies, targets and methods emerging and solidifying. Conflict in the Middle East – even before the 2026 US-Israel/Iran conflict – had shaped Australia's security from afar and increased the likelihood of politically motivated violence.

The security environment is deteriorating. While the national terrorism threat level remains within the PROBABLE band, the temperature in the environment is rising due to the threats from a growing mix of domestic and foreign actors – both religiously and ideologically motivated. Pervasive grievance narratives – amplified on social media – are lowering the threshold for lone-actor attacks and creating a climate that normalises intimidation, extremist symbolism and the use of violence.

Global terrorism threats are also likely to increase. Traditional groups such as Islamic State, al-Qa'ida and their affiliates are likely to increase their external operations capabilities, empowered by refreshed narratives and enabled by permissive geographic and online spaces. These groups continue to see Western interests across the globe as legitimate targets. Iran-aligned groups have undertaken a series of non-lethal attacks across Europe in early 2026. And in our near region, terrorism threats in South East Asia are at risk of re-emerging.

We expect spikes in the threat of communal violence directed at, or between, groups in the Australian community in response to domestic grievances. And, in our increasingly connected world, global events, overseas conflicts, and mis- and disinformation can also amplify the likelihood of communal violence.

Espionage and foreign interference remain at extreme levels, with great power competition in our region driving a relentless hunger for strategic advantage and an insatiable appetite for inside information. This manifests as the theft of privileged or sensitive information about government decision-making, defence capabilities, and intellectual property or cutting-edge research, especially when it has both military and civilian applications. To achieve their aims, foreign powers are seeking greater access to Australia's sensitive and classified information, and greater influence over Australian governments, decision-makers and public sentiment. These activities have a real cost. Espionage was conservatively estimated to have cost Australia $12.5 billion in 2023–24 – we judge these costs continue to be incurred. Looking ahead, we anticipate the threat of espionage and foreign interference will endure and intensify.

Nation states are increasingly operating in a security 'grey zone', using non-traditional tools to interfere in decision-making, promote discord and undermine social cohesion in Western democracies. Iran's orchestration of arson attacks against Jewish interests in Australia, while egregious, is not the only example of increasingly reckless and harmful activities by nation states to interfere in Australia. The degrading trajectory of our security environment and the growing willingness of regimes to undertake high-harm activity means there is a realistic possibility a foreign government will seek to undertake retribution against perceived dissidents in Australia.

Multiple countries will continue to relentlessly seek information about our military capabilities. AUKUS remains a priority target for intelligence collection and interference, including by some countries we consider friendly. Multiple nations will also continue to seek to covertly understand and shape Australia's politics and decision-making, our alliances and partnerships, and our economic and policy priorities. This includes trying to recruit government officials and interfering in our political processes at all levels of government, as well as monitoring, harassing and intimidating members of Australia's diaspora communities.

We are at the threshold for high-harm sabotage to impact Australia in the future. Authoritarian regimes are growing more willing to disrupt or destroy critical infrastructure to impede decision-making, damage the economy, undermine war-fighting capability, and sow social discord. Cyber is the most immediate vector for sabotage – it is low-cost, high-impact, deniable and scalable. We have seen highly sophisticated digital reconnaissance attempts to scan and penetrate critical infrastructure in Australia and other Five Eyes countries, targeting water, transport, telecommunications and energy networks. A destructive cyber attack could have severe and cascading impacts, including loss of life, if critical infrastructure and communications systems are degraded.

Hostile actors are adjusting their tactics, and Australia should be aware of the potential for these actors to use proxies – including criminals – to undertake actions on their behalf, creating plausible deniability while furthering their strategic intentions.

This could include state-sponsored or state-supported terrorism, or sabotage conducted by extremist or criminal proxies. Some unaffiliated individuals could also mobilise if they see it as advancing the interests of a foreign actor they favour over Australia. ASIO recognises this challenges traditional definitions, categorisations and assumptions, and we are adapting accordingly.

The future is uncertain and many of the driving factors of our security landscape are outside our control. But these challenges are not insurmountable or inevitable. Security is a shared responsibility and we will need to consider how Australia can collectively identify and counter threats. ASIO will use all of the tools we have available. ASIO will continue to adopt an aggressive operational posture to counter Australia's adversaries.

Technology advancement

The international drivers shaping Australia's security environment are being accelerated by rapid advances in technology. Social cohesion continues to be undermined by grievance narratives and conspiracy theories incubated via the internet. Social media algorithms can accelerate exposure to harmful and extreme content. ASIO holds concerns about the potential for artificial intelligence to exacerbate these trends by enabling online radicalisation driven by mis- and disinformation.

Permissive online environments and artificial intelligence tools can allow for capabilities, extremist ideologies, conspiracies and disinformation to be shared at unprecedented scale and speed. It can help extremists find and build relationships with other extremists more quickly and easily, help them communicate with one another more securely and enable attack planning and preparation. It can also expose people, particularly young people, to harmful and damaging extreme content and ideas.

Ubiquitous encryption is continuing to challenge our ability to identify and disrupt threats. End-to-end encryption impacts almost all of ASIO's priority counter-terrorism and counter-intelligence caseload, allowing security relevant activities to occur in secret, increasing the complexity of ASIO's operations and investigations.

Not all technological challenges are from cutting-edge, expensive sources – existing technology can produce new challenges as it becomes more affordable, effective, and widespread. For example, state and non-state adversaries are both increasingly exploiting small uncrewed aircraft systems for high-impact, low-cost attacks. This technology is cheap and readily available, and provides adversaries with a flexible, adaptable and affordable platform to inflict harm.

Some technologies are dual-use, with legitimate uses that can also be exploited. Artificial intelligence will allow adversaries to collect and analyse bulk data, enhancing their ability to target vulnerabilities in people, software and critical infrastructure to do harm. Artificial intelligence and other new technology will also facilitate foreign interference by allowing foreign adversaries to conduct more prolific, more credible and more effective disinformation campaigns.

In this environment, ASIO will continue to track and assess existing and emerging technological advancements, opportunities and challenges. ASIO will continue to use technology, including artificial intelligence, where it will enhance our capabilities to protect the security of Australians. Governed by strict ethical controls, with humans at the centre of decision-making, ASIO will ensure our lawful technical capabilities can help us detect and defeat threats to security.

Legislative and policy environment

In a more dynamic, diverse and degraded security environment, coupled with a rapidly evolving technological landscape, it is vital ASIO's legal framework remains fit-for-purpose to ensure we can continue to protect Australia and Australians.

Trust, governance, accountability and transparency are fundamental for achieving intelligence outcomes. The legal frameworks that govern ASIO's powers provide assurance to Ministers, Parliament and the public, that ASIO will use its powers lawfully, with propriety, and with due regard for the privacy of Australians.

ASIO must always balance the protection of Australians with the protection of their rights. These are complementary, not competing, priorities.

Community expectations

ASIO will rigorously and carefully prioritise our resources to ensure we remain well placed to protect Australia and Australians from threats to their security. Our powers are significant, which is why we must maintain the confidence and trust of the Australian people, by operating in proportion to the threats and in line with the standards and expectations of the Australian community.

Transparency and trust remain a key element of ASIO's agenda. Our governance processes guide us in achieving our mission and meeting public expectations of probity, accountability and transparency.

ASIO delivers on its mission using rigorous internal controls and embracing independent external oversight while ensuring ASIO is free from any influences or considerations not relevant to its functions.

Fiscal and labour market conditions

ASIO requires a dynamic, diverse and determined workforce.

We recognise the importance of attracting, developing and retaining our diverse, imaginative and curious workforce. We empower and support staff to achieve their full potential, fostering leadership at all levels.

ASIO recognises the importance of aligning our recruitment approach with Australia's employment and skills market. We continue to seek diverse skills for roles across our mission and enterprise, from intelligence analysts and technology specialists, to recruitment and finance officers.

Our people's agility, ingenuity, dedication and innovation allow us to keep pace with the threat environment, and we are always on the lookout for creative thinkers who want to make a difference.

Significant cost inflation in critical inputs to ASIO's capabilities and functions in areas such as cyber security, data analytics and enterprise technology will continue to stretch available resourcing. ASIO operates responsibly to deliver its outcomes by prioritising activity to fit within the funding provided by government.



Security intelligence outcomes

ASIO will achieve its purpose for the 2026–30 period through 4 key areas of focus, delivering security intelligence outcomes[1]:

1. Counter-intelligence
2. Counter-terrorism
3. Influence and impact
4. Top Secret–Privileged Access Vetting.

Counter-intelligence and counter-terrorism remain fundamental and enduring activities for ASIO.

Influence and impact continues to demonstrate the strategic importance we place on maximising the effect of our advice and insights so stakeholders can better understand, identify and manage sophisticated security threats.

The scale and sophistication of the threats facing Australia demands robust and resilient security settings. Vetting is a key component of this; only appropriately cleared people should have access to our nation's most sensitive information and assets.

The Top Secret–Privileged Access (TS-PA) Vetting Authority is delivering highly assured and transferable security clearances to Australia's highest-cleared workforce.

This capability enables the government to better manage and combat threats to its information, people and assets.

ASIO's performance against these 4 security intelligence outcomes will be measured through a combination of quantitative and qualitative methods, including defined targets, case studies, stakeholder feedback and identified milestones. ASIO will continue to progressively refine our performance measures to ensure we demonstrate our effectiveness in a transparent way, while safeguarding our sensitive capabilities and tradecraft.

Counter-intelligence

Espionage and foreign interference remain 2 of our 3 principal security concerns.

We will collect and analyse intelligence to quickly uncover and resolve threats to Australian Government, defence, political and other national interests. Over the period of this Corporate Plan, our advice will inform government decisions and actions to protect Australia and Australians from espionage and foreign interference. Our impactful and trusted advice to government, business, academia, industry and the public will raise awareness of the threat and establish a less permissive environment for covert actors. We will disrupt and deter those attempting to undermine our national interests, including through working with partners.

We will leverage our counter-intelligence capabilities to safeguard AUKUS, ensuring that this critical strategic partnership is resilient against foreign interference and espionage.

[1] Security intelligence outcomes Counter-intelligence, Counter-terrorism and Top Secret–Privileged Access Vetting correspond directly to the 'key activities' as referenced in the Portfolio Budget Statements, and Influence and impact relates to entity 'purpose', as defined under s16E(2) of the *Public Governance, Performance and Accountability Rule 2014*.

Counter-terrorism

ASIO protects Australia, its people and interests from politically motivated violence and the promotion of communal violence, in close cooperation with law enforcement and security partners. Politically motivated violence remains one of our principal security concerns.

We prioritise our resources against the greatest threats. While ASIO is not all-seeing and all-knowing and we cannot prevent every attack, our intelligence collection, investigation and assessment efforts within Australia and overseas enable ASIO to identify and counter terrorist threats; working with partners to strengthen public safety and intervene to disrupt attacks.

Over the period of this Corporate Plan, ASIO will continue to deliver influential, relevant and practical advice that has operational impact, hardens the environment, and informs government policy and responses to politically motivated violence and the promotion of communal violence. This includes participation in a national background checking scheme by providing security assessments for new and renewing firearms licence applicants.

Influence and impact

The scale and sophistication of the threats facing Australia requires ASIO to be proactive in its advice to government, business, academia, industry and the public.

ASIO will leverage our capabilities and insights to help stakeholders better understand, identify and manage security threats. We will promote security awareness and strengthen security maturity by providing expert insights and impactful advice.

Top Secret–Privileged Access Vetting

ASIO is delivering Australia's highest-level security clearances for the Commonwealth, protecting information, people and assets from insider threats now and into the future.

The TS-PA Vetting Authority provides a highly assured and transferable TS-PA clearance for Australia's most sensitive workforce, centralising the vetting process so that a single, trusted clearance can be used across agencies. By hardening access to the Government's critical resources and through leveraging ASIO's intelligence functions, the TS-PA Vetting Authority conducts a holistic, up-to-date assessment of each candidate's suitability, increasing the likelihood that insider threats will be detected and mitigated before compromise occurs.

Performance measure | Counter-intelligence

1. Impact of operational activities and security advice

Measure	The percentage of key stakeholders who confirm our counter-intelligence advice had a MEDIUM or HIGH impact on their decision-making in informing their activities, managing security risks, disrupting activities that threatened Australia's security, and/or informing government policy. Case studies which demonstrate the delivery of an operational counter-intelligence outcome.			
Targets (% and impact level)	2026–27	2027–28	2028–29	2029–30
	90% MEDIUM–HIGH > 1 MEDIUM–HIGH impact case study	90% MEDIUM–HIGH > 1 MEDIUM–HIGH impact case study	90% MEDIUM–HIGH > 1 MEDIUM–HIGH impact case study	90% MEDIUM–HIGH > 1 MEDIUM–HIGH impact case study
Rationale	ASIO's advice to partners within government, the national security community, industry and community sectors provides the knowledge and understanding that enables them to respond appropriately to security threats. Case studies demonstrate the depth and breadth of ASIO operational activity in understanding, disrupting and hardening the environment from espionage, foreign interference and sabotage, reducing harm to Australia and Australians.			
Methodology	Assessment of the impact of advice is drawn from examples of stakeholder feedback or case studies throughout the year, including the annual survey of key stakeholders. Stakeholders are: ■ drawn from relevant federal, state and territory governments, and private enterprise ■ ongoing, frequent recipients of ASIO counter-intelligence advice ■ engaged in relevant operational activities, managing security risks, disrupting espionage, foreign interference and sabotage activities that threaten Australia's security, and/or informing government policy. Assessment of the impact of operational activities is drawn from case studies which are provided at least twice a year for internal performance tracking. These case studies demonstrate the impact of ASIO's operational activities in disrupting and reducing the harm of espionage, foreign interference and sabotage. Case studies will be chosen early in the financial year on the basis of their potential to demonstrate the impact of operational activity, with consideration to protecting sensitive tradecraft, capabilities and information.			

Performance measure | Counter-terrorism

2. Impact of operational activities and security advice

Measure	The percentage of key stakeholders who confirm our counter-terrorism advice had a MEDIUM or HIGH impact on their decision-making in relation to informing their activities, managing security risks, disrupting activities that threatened Australia's security, and/or informing government policy. Case studies which demonstrate the delivery of an operational counter-terrorism outcome.			
Targets (% and impact level)	2026–27	2027–28	2028–29	2029–30
	90% MEDIUM–HIGH > 1 MEDIUM–HIGH impact case study	90% MEDIUM–HIGH > 1 MEDIUM–HIGH impact case study	90% MEDIUM–HIGH > 1 MEDIUM–HIGH impact case study	90% MEDIUM–HIGH > 1 MEDIUM–HIGH impact case study
Rationale	ASIO's advice to partners within government, the national security community, industry and community sectors provides the knowledge and understanding that enables them to respond appropriately to security threats. Case studies demonstrate the depth and breadth of ASIO operational activity in understanding, disrupting and hardening the environment from terrorism, reducing harm to Australia and Australians.			
Methodology	Assessment of the impact of advice is drawn from examples of stakeholder feedback or case studies throughout the year, including the annual survey of key stakeholders. Stakeholders are: ■ drawn from relevant federal, state and territory governments, and private enterprise ■ ongoing, frequent recipients of ASIO counter-terrorism advice ■ engaged in relevant operational activities, managing security risks, disrupting terrorism-related activities that threaten Australia's security, and/or informing government policy. Assessment of the impact of operational activities is drawn from case studies which are provided at least twice a year for internal performance tracking. These case studies demonstrate the impact of ASIO's operational activities in disrupting and reducing the harm of violent extremism. Case studies will be chosen early in the financial year on the basis of their potential to demonstrate the impact of operational activity, with consideration to protecting sensitive tradecraft, capabilities and information.			

Performance measure | Influence and impact

3. Delivery of impactful and influential Organisational activities and advice to stakeholders

Measure	Case studies which demonstrate the influence and impact of ASIO activities and advice, resulting in outcomes that contribute to protecting Australia and Australians from threats to their security. The percentage of key stakeholders who confirm the value of Organisational activities and advice to raise awareness of the security environment and how to counter threats.			
Targets (% and impact level)	2026–27	2027–28	2028–29	2029–30
	70% HIGH > 1 MEDIUM–HIGH impact case study	70% HIGH[2] > 1 MEDIUM–HIGH impact case study	70% HIGH[2] > 1 MEDIUM–HIGH impact case study	70% HIGH[2] > 1 MEDIUM–HIGH impact case study
Rationale	ASIO's advice to partners within government, the national security community, industry and community sectors enables them to respond appropriately to security threats. Case studies which leverage ASIO's capabilities and insights to help stakeholders better understand, identify and manage security threats.			
Methodology	Assessment of the impact of Organisational activities and advice is drawn from stakeholder feedback and case studies which are provided at least twice a year for internal performance tracking. Stakeholders are: ■ drawn from relevant federal, state and territory governments, and private enterprise ■ ongoing recipients of ASIO advice ■ engaged in relevant operational activities, managing security risks, and/or developing policies to protect Australia's security. These case studies demonstrate the impact of ASIO's activities and advice which contribute to protecting Australia and Australians from threats to their security. Case studies will be chosen early in the financial year on the basis of their potential to demonstrate the influence and impact of ASIO activities and advice, with consideration to protecting sensitive tradecraft, capabilities and information.			

[2] Targets will be reviewed following the development of the baseline in 2026–27.

Performance measure | Top Secret–Privileged Access Vetting

4. Top Secret–Privileged Access Vetting delivery

Measure	Metrics which demonstrate highly assured, transferable and timely security clearances are issued to Australia's highest-cleared workforce. Case studies which demonstrate the impact of TS-PA vetting delivery.
Targets (% and impact level)	2026–27 ■ < 4% of TS-PA cases on which quality assurance by the Quality Assurance Office is conducted require further assessment ■ 100% of requests to transfer sponsorship of existing, active and non-conditional TS-PA security clearances are processed without the need for a full reassessment ■ > 85% of routine, non-complex TS-PA security clearance decisions completed in 180 business days ■ > 85% of customer service engagements (calls and emails) resolved on first contact ■ > 95% availability of the Vetting Case Management Solution (VCMS), excluding scheduled downtime in support of digital user experience ■ > 90% of initial TS-PA clearance applications are conducted in VCMS ■ > 1 MEDIUM–HIGH impact case study 2027–28 to 2029–30 ■ Targets will be reviewed as TS-PA vetting matures throughout 2026–27
Rationale	ASIO is uplifting and hardening Australia's highest-level of security clearance to protect Australia's most sensitive resources, capabilities and information from the risk of compromise. The TS-PA Vetting Authority delivers a highly assured, consistent and transferable highest-level security clearance. A highly mobile TS-PA security cleared workforce will enable the Australian Government to respond rapidly to changes in Australia's strategic security environment and focus resources to deliver critical national security capabilities. Measures of vetting service delivery will highlight the growing maturity of ASIO's TS-PA vetting capability, while case studies demonstrate the role that TS-PA vetting plays in countering the insider threat.

Methodology	Quantitative Key Performance Indicators are used to assess the impact and growth of the TS-PA Vetting Authority as it progresses toward operational maturity. Quantitative assessment of vetting activities is informed by the independent audits of vetting compliance and consistency conducted by the Quality Assurance Office in the Office of National Intelligence; quarterly reporting to the Inspector-General for Intelligence and Security on clearance decisions exceeding 12 months; and customer service outcomes and feedback of the TS-PA Vetting Authority for routine cases, excluding cancellations. To safeguard the sensitivities associated with the size of the TS-PA clearance cohort across government, the total number of TS-PA decisions will be provided solely in the classified annex of ASIO's Annual Report, alongside the total number of delayed TS-PA security clearance decisions reported to the Inspector-General of Intelligence and Security during the reporting period. Case studies demonstrate the impact of TS-PA vetting activities in enabling the government to better manage and combat threats to its information, people and assets. Case studies are chosen on the basis of their potential to demonstrate the impact of vetting activity, with consideration to protecting sensitive tradecraft, capabilities and information.

Definitions

Advice impact definitions[3] – the definitions to be shared with key stakeholders when determining what level of impact our advice has had on their decision-making.

LOW	MEDIUM	HIGH
Our advice provided little or no context, and did not influence your decision-making.	Our advice provided context; was relevant and practical; and influenced your decision-making.	Our advice was timely and relevant; practical, focused and provided or enabled exercisable options; and directly informed and shaped your decision-making.

Advice – for the for the purposes of this performance framework, 'advice' encompasses all forms of communication – to the Australian Government, government agencies, and industry and community sector stakeholders – that conveys ASIO's expertise, intelligence, assessments, priorities and recommendations on security matters.

Influence and impact value definitions[4] – the definitions to be shared with key stakeholders when determining the value of ASIO activity to raise awareness of the security environment and advice on how to counter threats.

LOW	MEDIUM	HIGH
Advice was of limited value or not available.	Advice was adequate and available when required.	Advice was valuable to decision-making and readily available.

Case study impact definitions[5] – the assessment criteria for evaluation of case study impact.

LOW	MEDIUM	HIGH
The case study demonstrated context about the environment.	The case study demonstrated timely context to inform policy, security and/or an intelligence response to threats.	The case study demonstrated timely, actionable steps to directly mitigate high-harm threats.

[3] Advice impact definitions relate to counter-intelligence and counter-terrorism measures.
[4] Influence and impact value definition relates to the influence and impact measure.
[5] Case study impact definitions relate to counter-intelligence, counter-terrorism, influence and impact, and TS-PA measures.



Capabilities

ASIO's capabilities are our people, practices, partnerships, technology and assurance. ASIO continues to implement a range of strategies and plans to ensure we are continuing to evolve our capability in an effort to effectively and efficiently deliver on our purpose and undertake our key activities. The successful adoption of change associated with these strategies and plans will necessarily be underpinned by effective change management and consultation. ASIO operates in line with the APS Strategic Commissioning Framework. Core work is done in-house in most cases, and any outsourcing of core work is minimal and aligns with the limited circumstances permitted under the framework.



People

ASIO's people are fundamental to our business, and our culture enables their success. We recognise the importance of attracting, developing and retaining our diverse, imaginative and curious workforce. We empower and support staff to achieve their full potential, fostering leadership and accountability at all levels.

We invest in our people and planning to ensure the Organisation is well positioned to meet current and future workforce challenges. ASIO strives to reflect the society we protect – we do not discriminate against individuals on the basis of gender, sexual orientation, cultural background or ethnicity.



Practices

ASIO acts with authority to stay ahead of our adversaries through disciplined business processes and effective operational and analytical tradecraft. Our practices enable rigorous analysis, assessment and advice, intelligence-led and risk-based planning, operational decision-making, prioritisation, and ensure the effective and efficient use of resources. We adapt and lead in developing security practices, operating with integrity, proportionality and in compliance with the law.



Partnerships

Security is a shared responsibility and ASIO delivers its mission through strong partnerships. These relationships span government, including the National Intelligence Community, law enforcement, our state and territory partners, international counterparts, industry, academia and the Australian public. Partnerships are critical and we contribute our capabilities and experience to enhance the collective response to government.



Technology

ASIO uses a human-led, data-driven, technology-enabled approach to understand and respond to threats. We embrace new technologies, leverage automation and seize opportunities both to innovate and to uplift resilience, including working with Australian industry partners. We keep in step with rapidly changing technologies and practices to provide the security assurance Australians expect.



Assurance

Trust, governance, accountability and transparency are fundamental for achieving intelligence outcomes. Our risk, compliance and governance frameworks ensure we act within the letter and the spirit of the law. ASIO delivers on its mission using rigorous internal controls, embracing independent external oversight while ensuring ASIO is free from any influences or considerations not relevant to its functions.

Risk management and oversight

The Director-General is responsible for ensuring ASIO maintains an appropriate system of risk oversight and management to ensure ASIO can fulfil its purpose. Accepting and engaging with risk is inherent to ASIO's role of protecting Australia and Australians from threats to their security.

ASIO manages its risks through our enterprise risk management framework and corporate governance committees. ASIO's enterprise risk management framework seeks to embed risk management into the culture and work practices of the Organisation in order to maximise opportunities and manage uncertainty. ASIO engages with risk in all aspects of our business, and applies a sophisticated understanding of risk management practices to identify, evaluate and respond to risks and opportunities.

ASIO maintains compliance with all elements of the Commonwealth Risk Management Policy, demonstrating our commitment to an appropriate system of risk oversight and management.

The Executive Committee is ASIO's peak governing body, advising the Director-General on matters requiring executive decision-making. The Executive Committee's purpose is to provide oversight of all ASIO activities, including the effective management of ASIO's risks. The Executive Committee sets and reviews the Organisation's risk appetite and tolerance; determines whether ASIO's overall level of risk is acceptable; and considers whether the risk management framework remains effective.

The Executive Committee is supported in its consideration of ASIO's risk by the:

- Security and Compliance Committee, which makes recommendations to the Executive Committee on significant security and compliance matters relating to or impacting ASIO.
- Influence and Impact Committee, which makes recommendations to the Executive Committee on significant matters relating to or impacting on ASIO's influence agenda and gives account of performance against ASIO's objectives and endorsed lines of effort.
- Capability and Investment Committee, which makes recommendations to the Executive Committee on significant matters related to Organisational capability and investment, and ensures their alignment to ASIO's strategic objectives.
- Workforce Management Committee, which makes recommendations to the Executive Committee on significant Organisational workforce matters in line with ASIO's objectives, including the recruitment, retention and safety of ASIO's workforce.

The Audit and Risk Committee provides independent assurance and advice to the Director-General, including on ASIO's enterprise risk management framework and internal controls for the effective oversight of risks.


Audit and Risk Committee
(Quarterly)
Chaired by external member
Independent advisory committee to the Director-General on the appropriateness of ASIO's financial reporting, performance reporting, system of risk oversight and management, and the system of internal control for ASIO
Director-General of Security
Executive Committee
(Fortnightly)
Chaired by the Director-General of Security
Primary decision-making committee in ASIO
Security and Compliance Committee
(Monthly)
Chaired by Deputy Director-General Vetting Service Delivery
Primary advisory committee to the Executive Committee on organisational security and compliance matters
Influence and Impact Committee
(Monthly)
Chaired by Principal Advisor to the Director-General
Primary advisory committee to the Executive Committee on influence and impact matters
Capability and Investment Committee
(Monthly)
Chaired by Deputy Director-General Enterprise Service Delivery
Primary advisory committee to the Executive Committee on organisational capability and investment matters
Workforce Management Committee
(Bi-Monthly)
Chaired by Deputy Director-General Enterprise Service Delivery
Primary advisory committee to the Executive Committee on workforce matters

Key risks

ASIO faces a broad range of risks reflecting its responsibilities as Australia's security intelligence organisation. The risks arising from ASIO's work can be significant, but we are committed to engaging with risk to protect Australia and Australians from threats to their security.



Legal and propriety

Risks to compliance with laws, regulations, direction from government, international obligations, internal procedures or standards of propriety.



Financial

Risks to the security of money, assets and resources, including our financial sustainability.



Capability

Risks to the effectiveness and robustness of ASIO's capabilities, including technologies, data, facilities, partnerships, people and operational capabilities.



Health and safety

Risks to the health, safety and wellbeing of staff, partners, affiliates and the public.



Security

Risks to the protection of ASIO's capabilities, information and activities from compromise.



Reputation

Risks to the preservation of trust and confidence that government and the public place in ASIO.



asio.gov.au